

DIALOG(R)File 345:Inpadoc/Fam.& Legal Stat
(c) 2004 EPO. All rts. reserv.

18123608

Basic Patent (No,Kind,Date): JP 2002258975 A2 20020913 <No. of Patents:
001>

DEVICE FOR IDENTIFYING FINGERPRINT AND METHOD FOR THE SAME (English)

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE

Author (Inventor): ARAME TETSUO; AKISHINO KEIZO; OKI NOBUHIRO

IPC: *G06F-001/00; G06F-015/00; H04L-009/32

Language of Document: Japanese

Patent Family:

Patent No	Kind	Date	Applic No	Kind	Date
JP 2002258975	A2	20020913	JP 200152468	A	20010227 (BASIC)

Priority Data (No,Kind,Date):

JP 200152468 A 20010227

DIALOG(R)File 347:JAPIO

(c) 2004 JPO & JAPIO. All rts. reserv.

07390474 **Image available**

DEVICE FOR IDENTIFYING FINGERPRINT AND METHOD FOR THE SAME

PUB. NO.: 2002-258975 [JP 2002258975 A]

PUBLISHED: September 13, 2002 (20020913)

INVENTOR(s): ARAME TETSUO

AKISHINO KEIZO

OKI NOBUHIRO

APPLICANT(s): NIPPON TELEGRAPH & TELEPHONE EAST CORP

APPL. NO.: 2001-052468 [JP 200152468]

FILED: February 27, 2001 (20010227)

INTL CLASS: G06F-001/00; G06F-015/00; H04L-009/32

ABSTRACT

PROBLEM TO BE SOLVED: To provide a fingerprint identifying device capable of strengthening the identification (confirmation) of a person himself or herself, and preventing any danger for infringement of his or her privacy.

SOLUTION: A user inserts an IC card 14 in which the fingerprint data of the user himself or herself and a log-on ID are preliminarily stored into a reading/identifying device 15, and allows the device 15 to read the

fingerprint picture of the user himself or herself from a fingerprint reading screen 15a of the device 15. The device 15 collates the fingerprint picture of the user with the fingerprint data of the user stored in the IC card 14, and when they coincide with each other, the device 15 reads the log-on ID from the IC card 14. A task terminal 11 receives the result of the fingerprint identification and the log-on ID (when the identification is successful) from the device 15, and when the received log-on ID coincides with a log-on ID stored in a storage device 13, the task terminal 11 permits the user to use the task terminal.

COPYRIGHT: (C)2002, JPO

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号
特開2002-258975
(P2002-258975A)

(43)公開日 平成14年9月13日(2002.9.13)

(51)Int.Cl. ⁷	識別記号	FI	マーク(参考)
G 0 6 F 1/00	3 7 0	G 0 6 F 1/00	3 7 0 E 5 B 0 8 5
15/00	3 3 0	15/00	3 3 0 F 5 J 1 0 4
			3 3 0 G
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 E
			6 7 3 D
審査請求 未請求 請求項の数3 OL (全 5 頁)			

(21)出願番号 特願2001-52468(P2001-52468)

(22)出願日 平成13年2月27日(2001.2.27)

(71)出願人 399040405

東日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号

(72)発明者 新目 徹夫

東京都新宿区西新宿三丁目19番2号 東日
本電信電話株式会社内

(72)発明者 秋篠 敬三

東京都新宿区西新宿三丁目19番2号 東日
本電信電話株式会社内

(74)代理人 100064908

弁理士 志賀 正武

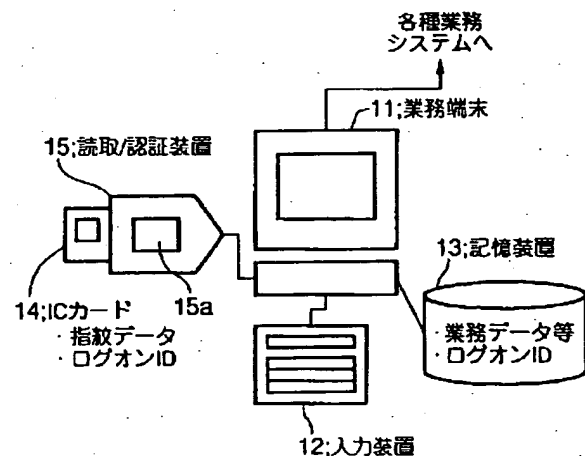
最終頁に続く

(54)【発明の名称】 指紋認証装置および指紋認証方法

(57)【要約】

【課題】 従来以上に本人の認証(確認)を強化することができ、しかも、プライバシーの侵害の虞れがない指紋認証装置を提供する。

【解決手段】 ユーザは、自身の指紋データとログオンIDが予め記憶されたICカード14を読取/認証装置15に挿入し、そして、読取/認証装置15の指紋読取面15aから自身の指紋画像を読み込ませる。読取/認証装置15は、ユーザの指紋画像と、ICカード14に記憶されたユーザの指紋データとを照合し、一致した場合はICカード14からログオンIDを読み出す。業務端末11は、読取/認証装置15から指紋認証の結果と、認証が成功した場合はログオンIDを受け取り、受け取ったログオンIDが記憶装置13内に記憶されているログオンIDと一致した場合に、ユーザに対して業務端末の利用を許可する。



【特許請求の範囲】

【請求項1】 ユーザの指紋データおよび識別番号が記憶されたカードと、

前記ユーザの識別番号が記憶された記憶手段と、

前記ユーザの指紋を読み取る指紋読取手段と、

前記カードの指紋データおよび識別番号を読み取る読取手段と、

前記カードから読み取られた指紋データと前記指紋読取装置によって読み取られたユーザの指紋とを比較し、両者が一致しているか否かを判定する第1の認証手段と、前記カードから読み取られた識別番号と前記記憶手段内の識別番号とを比較し、両者が一致しているか否かを判定する第2の認証手段と、

を具備し、前記第1、第2の認証手段による認証結果が共に「一致している」であった場合に認証結果が良であると判定することを特徴とする指紋認証装置。

【請求項2】 前記記憶手段および前記第2の認証装置を前記第1の認証装置に対し遠隔地に設け、両者間を通信回線で接続したことを特徴とする請求項1に記載の指紋認証装置。

【請求項3】 ユーザの指紋を取得する第1の処理と、ユーザのカードから指紋データを取得する第2の処理と、ユーザの指紋と前記指紋データとを比較し、両者が一致しているか否かを判定する第3の処理と、前記第3の処理の判定結果が一致であった場合に、前記カードから識別番号を読み取る第4の処理と、該識別番号と記憶手段内に予め記憶されている識別番号とを比較し、両者が一致しているか否かを判定する第5の処理と、前記第5の処理による判定結果が「一致」であった場合に、認証結果が良であると判定することを特徴とする指紋認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、システムログオン時にユーザ認証を行う認証装置に係り、特に、ICカードに記憶された電子データの読取りと、指紋読取りとに基づいて認証を行う指紋認証装置および指紋認証方法に関する。

【0002】

【従来の技術】 従来、システムログオン時にユーザ認証を行う方法として、①ユーザが暗証番号やパスワードを入力する、②ユーザがカード読み取り器にカードを挿入し、読み取り器がカード上に取り付けられた媒体の磁気／電子データを読み取ってデータベースと照合することで本人確認を行う、③ユーザの指紋を照合する等の方法が知られている。

【0003】 図3は、従来のユーザ認証方法を説明するためのシステム構成例を示す図であり、ユーザは業務端

末1を利用する際に、入力装置（キーボード）2から暗証番号／パスワードを入力する。業務端末1は入力装置2からの入力されたデータと、予め記憶装置3に記憶されている認証データとを照合し、一致した場合に、ユーザに対して業務端末1の利用を許可する。この場合、正規のユーザに与えられる暗証番号／パスワードが不正に第三者に知られた場合、業務端末1を不正利用される恐れがある。

【0004】 これに対し、指紋認証による場合、ユーザは業務端末1を利用する際に、指紋読取装置4によって指紋画像を読み込ませる。業務端末1は指紋読取装置4によって読取った指紋画像と、記憶装置3に記憶されている指紋データとを照合し、一致した場合に、ユーザに対して業務端末1の利用を許可する。この場合、記憶装置3の指紋データが不正に第三者に漏洩した場合、プライバシーの侵害になるため、ユーザが記憶装置3への指紋データの登録に抵抗を示すことがある。また、利用する業務端末全てにユーザの指紋データを登録する必要があり、運用が複雑になる欠点がある。

【0005】 図4は、従来のユーザ認証を説明するための他のシステム構成例を示す図である。ユーザは、業務端末5を使用する際に、指紋読取装置6から指紋画像を読み込ませる。業務端末5は指紋読取装置6によって読取った指紋画像を、通信回線7を経由して業務サーバ8へ送信する。業務サーバ8は、その指紋画像と記憶装置9に格納された指紋データとを照合し、照合結果を通信回線7を介して業務端末5へに返送する。業務端末5は業務サーバ8からの結果を受けて、指紋認証が成功した場合にはユーザに業務端末5の利用を許可する。この方法の場合、ユーザが別の業務端末を使用する場合に、指紋データを再登録する必要はないが、記憶装置9の指紋データが流出した場合、多数のユーザに対してプライバシーの侵害が発生する問題がある。

【0006】

【発明が解決しようとする課題】 上述したように、暗証番号やパスワードあるいはカードによる認証の場合、盗難により本人以外の者が不正に業務システムを利用してしまふ虞れがあり、一方、指紋による認証の場合、指紋データが流出した時にプライバシーが侵害される虞れがあることから、ユーザにとって事前の指紋登録に対して心理的な抵抗があるという欠点がある。

【0007】 この発明は、このような事情を考慮してなされたもので、その目的は、従来以上に本人の認証（確認）を強化することができ、しかも、プライバシーの侵害の虞れがない指紋認証装置および指紋認証方法を提供することにある。

【0008】

【課題を解決するための手段】 この発明は上記の課題を解決すべくなされたもので、請求項1に記載の発明は、ユーザの指紋データおよび識別番号が記憶されたカード

と、前記ユーザの識別番号が記憶された記憶手段と、前記ユーザの指紋を読み取る指紋読取手段と、前記カードの指紋データおよび識別番号を読み取る読取手段と、前記カードから読み取られた指紋データと前記指紋読取装置によって読み取られたユーザの指紋とを比較し、両者が一致しているか否かを判定する第1の認証手段と、前記カードから読み取られた識別番号と前記記憶手段内の識別番号とを比較し、両者が一致しているか否かを判定する第2の認証手段とを具備し、前記第1、第2の認証手段による認証結果が共に「一致している」であった場合に認証結果が良であると判定することを特徴とする指紋認証装置である。

【0009】また、請求項2に記載の発明は、請求項1に記載の指紋認証装置において、前記記憶手段および前記第2の認証装置を前記第1の認証装置に対し遠隔地に設け、両者間を通信回線で接続したことを特徴とする。また、請求項3に記載の発明は、ユーザの指紋を取得する第1の処理と、ユーザのカードから指紋データを取得する第2の処理と、ユーザの指紋と前記指紋データとを比較し、両者が一致しているか否かを判定する第3の処理と、前記第3の処理の判定結果が一致であった場合に、前記カードから識別番号を読み取る第4の処理と、該識別番号と記憶手段内に予め記憶されている識別番号とを比較し、両者が一致しているか否かを判定する第5の処理と、前記第5の処理による判定結果が「一致」であった場合に、認証結果が良であると判定することを特徴とする指紋認証方法である。

【0010】

【発明の実施の形態】以下、図面を参照し、この発明の実施の形態について説明する。図1はこの発明の第1の実施の形態による指紋認証装置を適用したシステムの構成を示すブロック図であり、この図において、11は業務端末、12は入力装置、13は記憶装置である。この記憶装置13には、予め、業務端末11を使用するユーザのログオンIDが記憶されている。14はユーザが所有するICカードであり、所有者のログオンIDおよび指紋データが記憶されている。15はICカード14を読み取る読取装置、指紋を読み取る指紋読取装置および指紋照合を行う認証装置の機能を有する読取/認証装置である。

【0011】このような構成において、ユーザは、業務端末11を利用する際にユーザの指紋データとログオンIDが予め記憶されたICカード14を読取/認証装置15に挿入し、そして、読取/認証装置15の指紋読取面15aから指紋画像を読み込ませる。一方、業務端末11は読取/認証装置15に対して、指紋認証結果とログオンIDを要求する。読取/認証装置15は、ユーザの指紋画像と、ICカード14に記憶されたユーザの指紋データとを照合し、一致した場合はICカード14からログオンIDを読出す。業務端末11は、読取/認証

装置15から指紋認証の結果と、認証が成功した場合はログオンIDとを受け取り、受け取ったログオンIDが記憶装置13内に記憶されているのログオンIDと一致した場合に、ユーザに対して業務端末の利用を許可する。

【0012】上記実施形態によれば、ICカード14内の電子データのチェックと、指紋認証により、セキュリティの強化を図ることができる。また、指紋照合時に使用するユーザの指紋データは、個人が保持しているもので、プライバシーの保護を図ると共に、別の業務端末を利用する場合にも指紋データを再登録する必要がない利点がある。また、本実施形態は構成が単純であり、かつ、照合機能も備えていることから、既存の業務端末に組み込むことが容易である。

【0013】次に、この発明の第2の実施形態について説明する。図2は同実施形態による指紋認証装置を適用したシステムの構成を示すブロック図であり、この図において、21は業務端末である。24はユーザが所有するICカードであり、上記第1の実施形態と同様に、所有者のログオンIDおよび指紋データが記憶されている。25は上述した読取/認証装置15と同様に構成された読取/認証装置である。26は通信回線、27は業務サーバ、28は業務サーバ27によって書込/読出が行われる記憶装置である。この記憶装置23には、予め、業務端末21を使用するユーザのログオンIDが記憶されている。

【0014】このような構成において、ユーザは業務端末21を利用する際に、ユーザの指紋データとログオンIDを保持したICカード24を読取/認証装置25に挿入し、指紋読取面25aから自身の指紋画像を読み取らせる。業務端末21は読取/認証装置25に対して、指紋認証とログオンIDを要求する。読取/認証装置25はユーザの指紋画像と、ICカード24に記憶されたユーザの指紋データとを照合し、一致した場合はICカードからログオンIDを読出す。業務端末21は、読取/認証装置25から認証結果と、認証が成功した場合はログオンIDを受け取り、受け取ったログオンIDを通信回線26を介して業務サーバ27へ送信する。業務サーバ27は受け取ったログオンIDと記憶装置28内のログオンIDとを照合し、その結果を通信回線26を介して業務端末21に返送する。業務端末21は照合結果が一致していた場合、ユーザに対して業務端末21の利用を許可する。

【0015】上述した第2の実施形態によれば、ユーザ個人が所有するICカード内に指紋データを格納することから、カードの盗難があった場合でも、そのカード所有者以外の指紋データが流出する危険を回避することができる。また、本実施形態を用いると、既存の業務システムに別途指紋データ共用装置等を用意することなく、容易に指紋認証によるログオン方式を組み込むことが可

能となる利点がある。

【0016】

【発明の効果】以上説明したように、この発明によれば、既存の暗証番号・パスワード入力方式や、カード上の媒体から磁気／電子データを読み取る方式に比較し、本人性確認が強化され、業務システムのユーザに対するセキュリティが向上する効果が得られる。また、業務システム端末や、業務システムのデータベース内に指紋データを保持すると、流出する危険性があるが、そのような危険を排除することができ、プライバシー保護を図ることができる。また、磁気カード読取り装置と指紋読取装置を一体化し、装置に指紋照合機能を持たせることで、装置の小型化を図ることが出来ると共に、演算能力の低い端末（一般のパーソナルコンピュータ等）への組み込み用途としても最適であり、既存の業務システムのセキュリティ強化を図ることが出来る。

【図面の簡単な説明】

【図1】 この発明の第1の実施形態の構成を示すブロック図である。

【図2】 この発明の第2の実施形態の構成を示すブロック図である。

【図3】 従来のユーザ認証方法を説明するためのシステム構成例を示す図である。

【図4】 従来のユーザ認証方法を説明するための他のシステム構成例を示す図である。

【符号の説明】

11、21…業務端末

13…記憶装置

14、24…ICカード

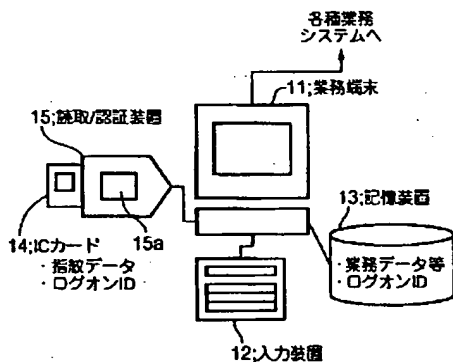
15、25…読取／認証装置

26…通信回線

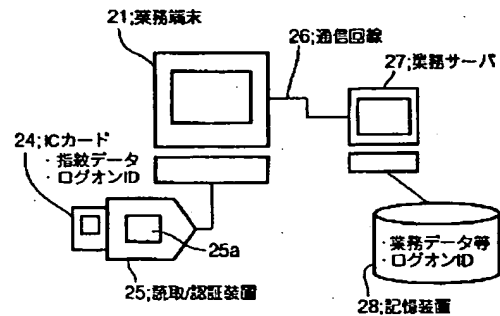
27…業務サーバ

28…記憶装置。

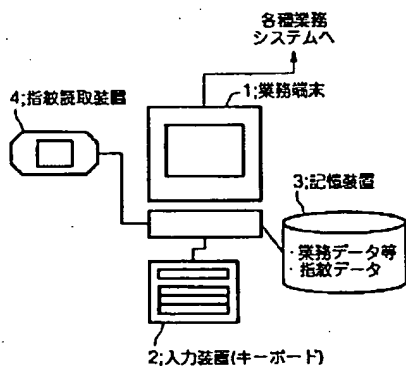
【図1】



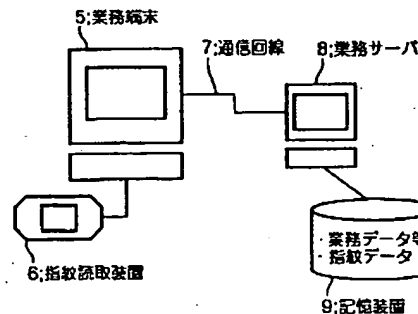
【図2】



【図3】



【図4】



フロントページの続き

(72)発明者 沖 宣宏

東京都新宿区西新宿三丁目19番2号 東日
本電信電話株式会社内

Fターム(参考) 5B085 AE12 AE23 AE26 BC01
5J104 AA07 KA01 KA17 NA05 NA35
NA38 NA41 PA07